WinSCP + PuTTY as an alternative to F-Secure
July 11, 2006

Brief Summary of this Document

F-Secure SSH Client 5.4 Build 34 is currently the Berkeley Lab's standard SSH client. It consists of three integrated components: F-Secure SSH Terminal, F-Secure SSH Tunnel, and F-Secure SSH File Transfer. The most recent version of this program is now developed by AttachmateWRQ under the name Reflection for Secure IT. The new version was not received well by lab customers who preferred to remain on the older and still functioning version. As a result, the maintenance contract with F-secure was dropped. The Berkeley Lab currently has a license for F-Secure SSH Client 5.4 Build 34, which is available on the Lab's download page. This program will remain on the download page until a serious flaw is found in it that will force us to convert to an alternative. The combination of WinSCP and PuTTY is as functional as F-Secure SSH Client with a few minor differences, but should be an acceptable alternative if we are ever forced to discontinue our use of F-Secure's SSH Client.

Background Information

WinSCP is an open source freeware SFTP client for Windows using SSH. Legacy SCP protocol is also supported. Its main function is safe copying of files between a local and a remote computer.

PuTTY is a free implementation of Telnet and SSH for Win32 and UNIX platforms, along with an `xterm` terminal emulator. **putty-0.58-installer.exe** installs all of its files into **C:\Program Files\PuTTY**. Here is a list of what comes with **putty-0.58-installer.exe**:

- **PuTTY** is a free (MIT-licensed) Win32 Telnet and SSH client. This tool opens a GUI to change PuTTY's configuration. Each session is opened in its own window from which additional sessions can be opened.
- **PSCP**, the PuTTY Secure Copy client, is a command line tool for transferring files securely between computers using an SSH connection.
- **PSFTP**, the PuTTY SFTP client, is a command line tool for transferring files securely between computers using an SSH connection.
- **Plink** (PuTTY Link) is a command-line connection tool similar to UNIX SSH. It is primarily used for automated operations, such as making CVS access a repository on a remote server. Plink is probably not what you want if you want to run an interactive session in a console window.
- **PuTTYgen** is a key generator which uses a GUI to generate pairs of public and private keys to be used with PuTTY, PSCP, and Plink, as well as the PuTTY authentication agent, Pageant. PuTTYgen generates RSA and DSA keys. This program is also included with WinSCP.
- **Pageant** is an SSH authentication agent. It holds your private keys in memory, already decoded, so that you can use them often without needing to type a passphrase. This tool can be used from the command line or with a GUI. This program is also included with WinSCP.

Reasons for converting from F-Secure to WinSCP+PuTTY

- If a critical flaw is found in F-Secure SSH Client 5.4 Build 34, then we will consider converting to WinSCP and PuTTY.
- If an important or desirable new feature is introduced that is not available in the Berkeley Lab's current version of F-Secure SSH Client, then we will consider converting to WinSCP and PuTTY.
- The new version of F-Secure SSH Client has been deemed unacceptable and not worth investing into. WinSCP and PuTTY have been offered as an alternative because they are both open-source and will save the lab money.
- The Berkeley Lab has paid for a license for F-Secure SSH Client 5.4 Build 34 which can be downloaded from the Lab's download page. It will remain as the Lab's default SSH client until something forces us to change to an alternative such as WinSCP and PuTTY.

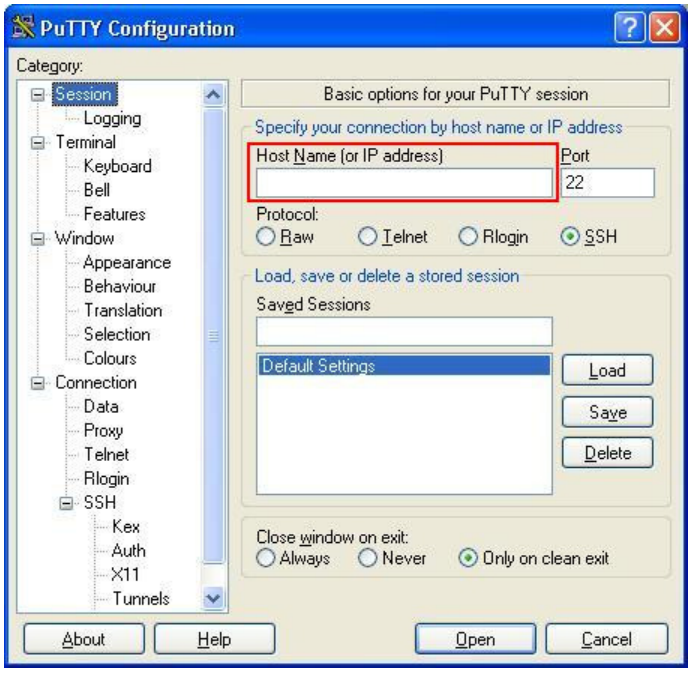
Differences between WinSCP+PuTTY and F-Secure

- WinSCP has an interface similar to an FTP program. On the other hand, F-Secure's interface is more like a combination of explorer and FTP interfaces.
- WinSCP does not have a Tunnel View Window similar to F-Secure. PuTTY can be used to setup tunnels instead.
- The terminal program that WinSCP provides seems very limited when compared to F-Secure's SSH terminal. PuTTY can be opened from WinSCP to provide a terminal similar to F-Secure's.
- Opening another terminal with PuTTY is not as simple as clicking an icon in F-Secure because PuTTY does not save your password. If your means of authentication is a password, then you will have to at least provide your password each time a PuTTY session is opened. If your means of authentication is with a public/private key pair, then you can use Pageant to provide your passphrase to PuTTY for each session that is opened.
- By default, you will have to enter your password or passphrase every time a PuTTY session is opened from WinSCP. However, this can be configured so that you will not have to re-authenticate yourself.

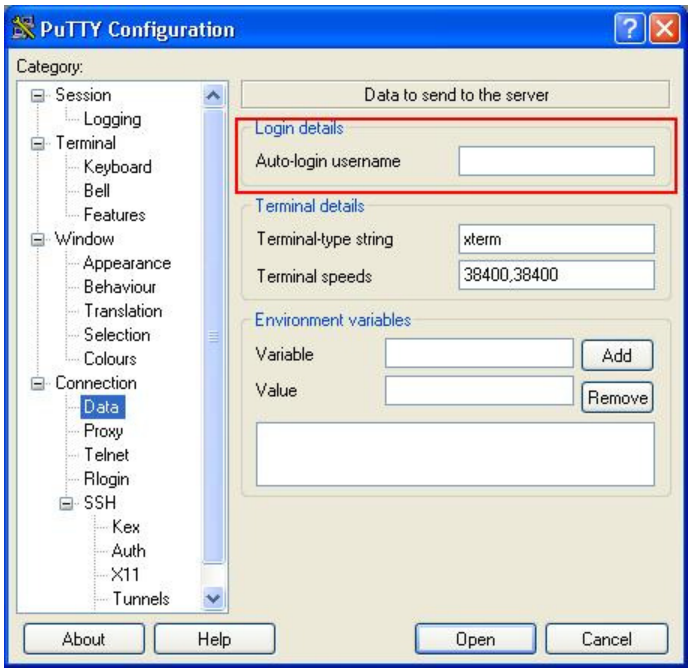
How to Configure PuTTY SSH Client

PuTTY can be used by itself to connect to a remote computer using SSH, or it can be used in conjunction with WinSCP. Creating the settings in PuTTY is nearly identical to setting them up in F-Secure.

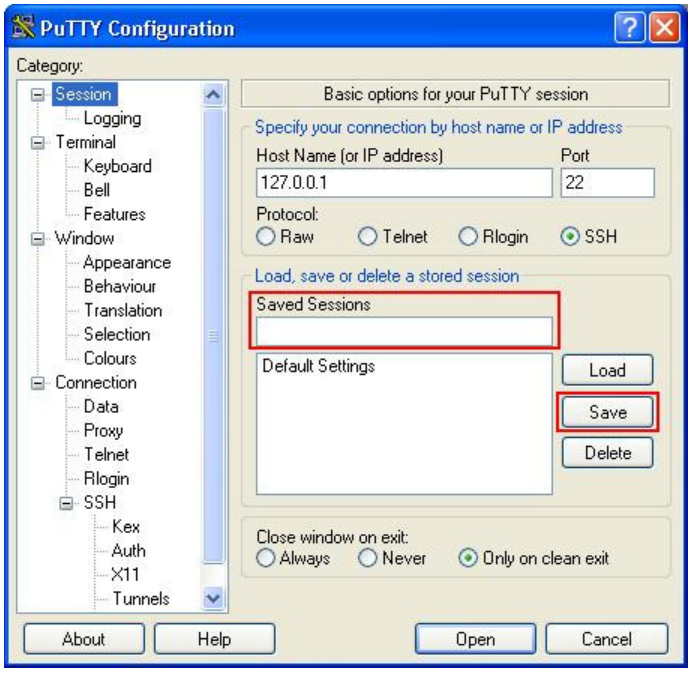
1. Open **PuTTY**. (Double-click the **PuTTY icon** on your desktop or go to **Start → Programs or All Programs → PuTTY → PuTTY**)
2. With **Session** selected on the left, fill in **Host Name (or IP Address)** information.



3. Now select **Connection → Data** from the left and fill in your username under **Autologin-username**.



4. To save your settings, go back to the **Session** category and type in a name for your session under **Saved Sessions**. Then click the **Save** button.



5. To start your session, click on the **Open** button at the bottom right of the configuration window.

★ **Notes on PuTTY**:

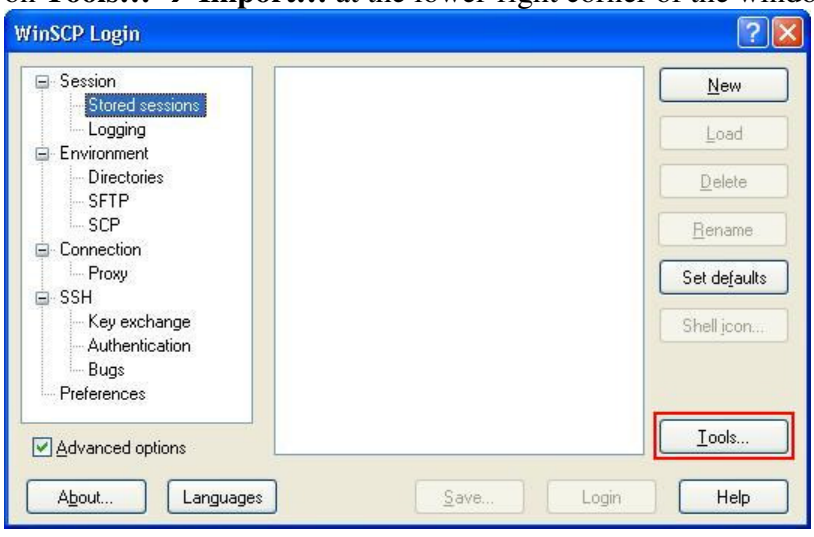
- PuTTYgen is used to create encryption keys for PuTTY and for WinSCP. It is included in installers of both programs.
- PuTTY must be installed separately from WinSCP in order to use PuTTY SSH.
- Multiple sessions can be opened by clicking on the PuTTY icon at the top left corner of the PuTTY session window and selecting either **New Session…**, **Duplicate Session**, or **Saved Sessions**.
- Pageant can help you save time from re-entering your passphrase.
- **X11 Forwarding** can be set in the **PuTTY Configuration** window under **Connection → SSH → X11**.

For further information about **How to Secure an X11 Windows Server**, go to the following link: http://isolate.lbl.gov/openXserver.htm.

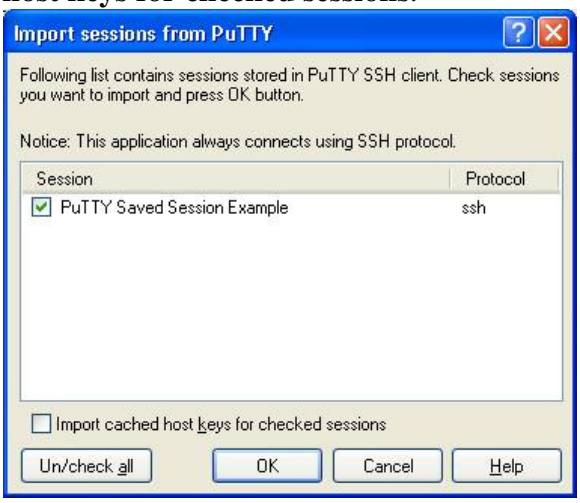
- **SSH tunnels** can be set in the **PuTTY Configuration** window under **Connection → SSH → Tunnels**.

How to Configure WinSCP

1. Open **WinSCP3**. (Double-click the **WinSCP3 icon** on your desktop or go to **Start → Programs or All Programs → WinSCP3 → WinSCP**)
2. The **WinSCP Login** window will appear. To save some time from entering the same settings again, you can import your PuTTY settings. If you do not have any saved PuTTY sessions, then skip to **Step 3**.
   a. To import a saved PuTTY session go to **Session → Stored Sessions** on the left side and click on **Tools… → Import…** at the lower-right corner of the window.



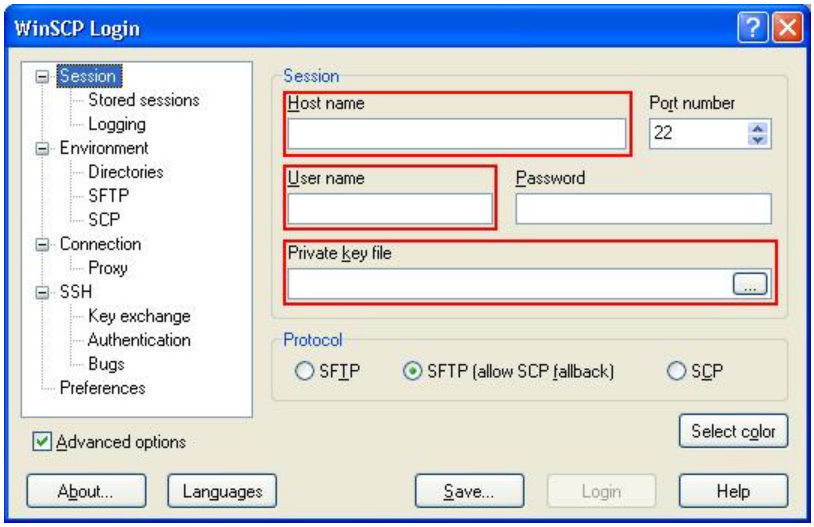
b. The **Import sessions from PuTTY** window will open. Put a checkmark next to the saved PuTTY sessions that you would like to import. Note that there is also an option to **Import cached host keys for checked sessions**.



c. Click **OK** to import your PuTTY settings.

d. Skip to **Step 5**.

3. Click on **Session** from the left side. Then fill in the fields for **Host name** and **User Name**.



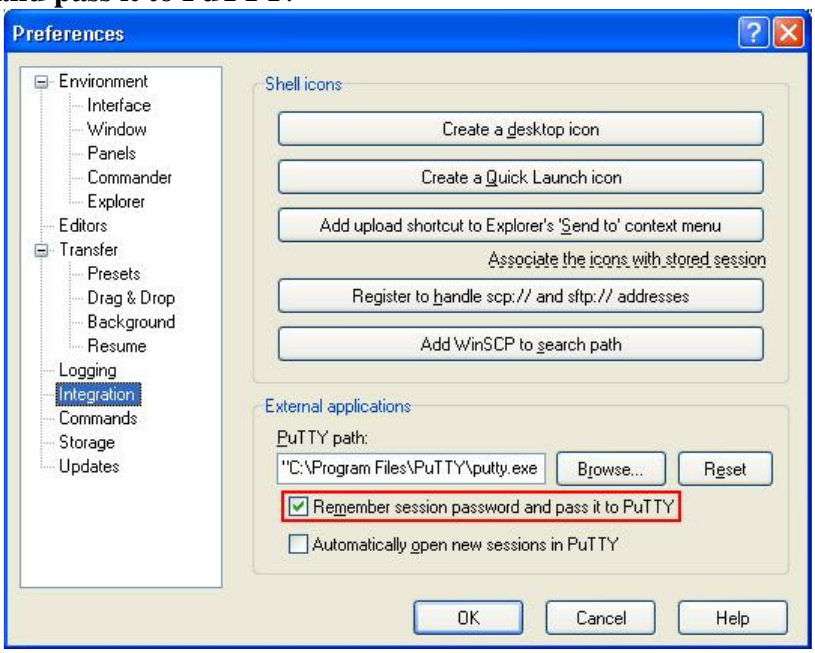
4. If you have a private key file that was created using PuTTYgen, then you can use the **…** button under **Private key file** to open that file.
5. To save your settings, click on the **Save…** button at the bottom of the window. Note that this button is grayed out under **Session → Stored sessions**.
6. Click the **Login** button at the bottom of the window to connect with your new saved session.

★ **Notes on WinSCP:**

- The SSH terminal that WinSCP provides does not have the same feel as a terminal on a UNIX/Linux system. For example, commands entered on WinSCP's terminal cannot be TAB-completed. An alternative to this terminal is PuTTY, which can be opened from WinSCP but must be installed separately. To open PuTTY from WinSCP go to

Commands → Open in PuTTY, press **CTRL+P**, or click the PuTTY icon on the toolbar.

- By default, WinSCP will create a PuTTY session file called **WinSCP temporary session**. The settings for this session can be altered by using the **PuTTY configuration** window.
- WinSCP will open the PuTTY session file with the same name as the current WinSCP session. If a PuTTY session does not exist, then PuTTY will be opened with the **WinSCP temporary session** file.
- While WinSCP is connected, it is possible to open several PuTTY sessions without retyping your password. To do this, go to **Options → Preferences** or press **CTRL+ALT+P**. On the left side of the **Preferences** window select **Integration**. Under **External Applications** on the right, place a checkmark next to **Remember session password and pass it to PuTTY**.



Note that WinSCP will only pass your session password to PuTTY sessions opened through WinSCP.

- WinSCP and PuTTY can both use Pageant to store unencrypted private keys.

About PuTTY Secure FTP (PSFTP)

The PuTTY version of SFTP is **PSFTP**. From the command prompt, it is easier to execute psftp.exe and any of the other commands included in the PuTTY installer by adding the location of the PuTTY directory to the PATH environment variable. There are two ways to do this:

1. Each time you open a Windows command prompt, enter **set PATH=C:\Progra~1\PuTTy;%PATH%**.
2. Or, **Right-click on My Computer → Properties → Advanced → Environment Variables** and edit **PATH** under **System variables** by adding **;C:\Progra~1\PuTTY** at the end of its **Variable value**.

After adding the path to PuTTY, the commands can be executed from any folder.

Here is a list of the command's **Usage** and **Options**:

C:\>psftp -h

PuTTY Secure File Transfer (SFTP) client
Release 0.58
Usage: psftp [options] [user@]host
Options:

-V	print version information and exit
-pgpfp	print PGP key fingerprints and exit
-b file	use specified batchfile
-bc	output batchfile commands
-be	don't stop batchfile processing if errors
-v	show verbose messages
-load sessname	Load settings from saved session
-l user	connect with specified username
-P port	connect to specified port
-pw passw	login with specified password
-1 -2	force use of particular SSH protocol version
-4 -6	force use of IPv4 or IPv6
-C	enable compression
-i key	private key file for authentication
-batch	disable all interactive prompts

Here is a list of the **commands** available at the psftp command prompt:

psftp> help

!	run a local command
bye	finish your SFTP session
cd	change your remote working directory
chmod	change file permissions and modes
close	finish your SFTP session but do not quit PSFTP
del	delete files on the remote server
dir	list remote files
exit	finish your SFTP session
get	download a file from the server to your local machine
help	give help
lcd	change local working directory
lpwd	print local working directory
ls	list remote files
mget	download multiple files at once
mkdir	create directories on the remote server
mput	upload multiple files at once
mv	move or rename file(s) on the remote server
open	connect to a host
put	upload a file from your local machine to the server
pwd	print your remote working directory

quit	finish your SFTP session
reget	continue downloading files
ren	move or rename file(s) on the remote server
reput	continue uploading files
rm	delete files on the remote server
rmdir	remove directories on the remote server